PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-124178
(43)Date of publication of application : 06.05.1994

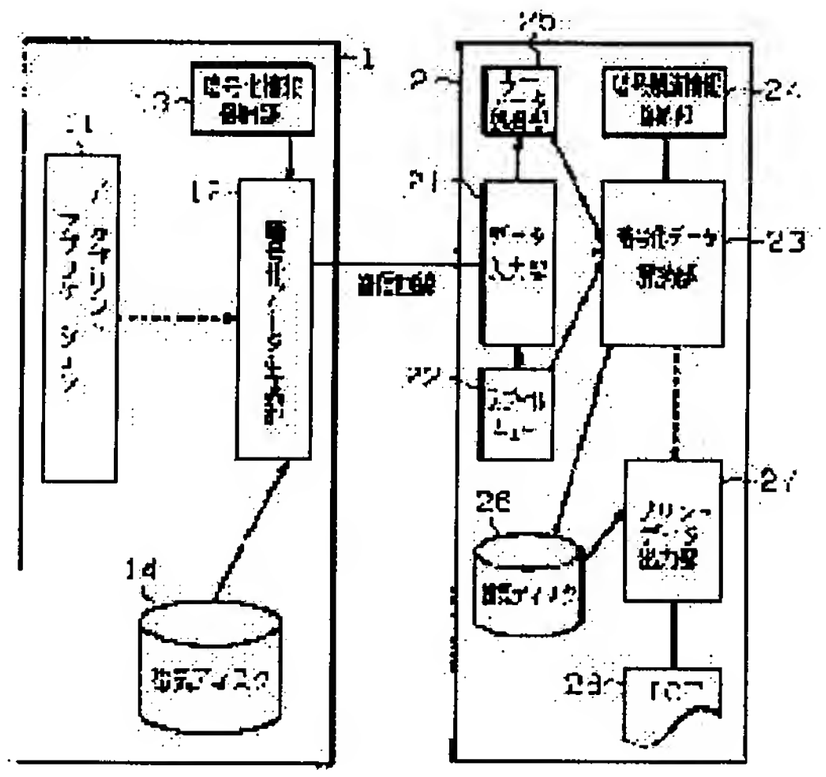
(51)Int.Cl. G06F 3/12
B41J 2/485
B41J 5/30
G06F 12/14

(21)Application number : 04-300383
(22)Date of filing : 13.10.1992

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : YOMOGIZAWA MITSUHISA

(54) SECURITY SYSTEM FOR PRINT DATA

(57)Abstract:
PURPOSE: To exactly ensure security by preventing the content of security objective data existing in a spool queue from being known even when the third person tries to look in at the security objective data through a display or the like.
CONSTITUTION: A print data preparing device 1 is equipped with a ciphered data preparing part 12 which ciphers print data, adds a user ID, key code, and ciphered ID to the ciphered data, and transfers the data to a printer side. A printer 2 is equipped with a ciphered data deciphering part 23 which deciphers the ciphered data based on the user ID or the like. The ciphered data transferred to the printer 2 are temporarily stored in a spool queue 22, and at the time of printing, the ciphered data are deciphered by the ciphered data deciphering part 23, and outputted, only when a pass word is matched. The ciphered data are stored in the spool queue 22, so that only the lump of the meaningless data can be seen even when the third person tries to look in at the content, and the content of the print data can be prevented from being known.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－124178

(43)公開日　平成６年(1994)５月６日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	3/12		A		
Ｂ４１Ｊ	2/485				
	5/30		Z　8703－2C		
Ｇ０６Ｆ	12/14	３２０	B　9293－5B		
			8703－2C	Ｂ４１Ｊ　3/12	Z

審査請求　未請求　請求項の数１(全　９　頁)

(21)出願番号　特願平4－300383

(22)出願日　平成４年(1992)10月13日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　蓬沢　光久
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社内

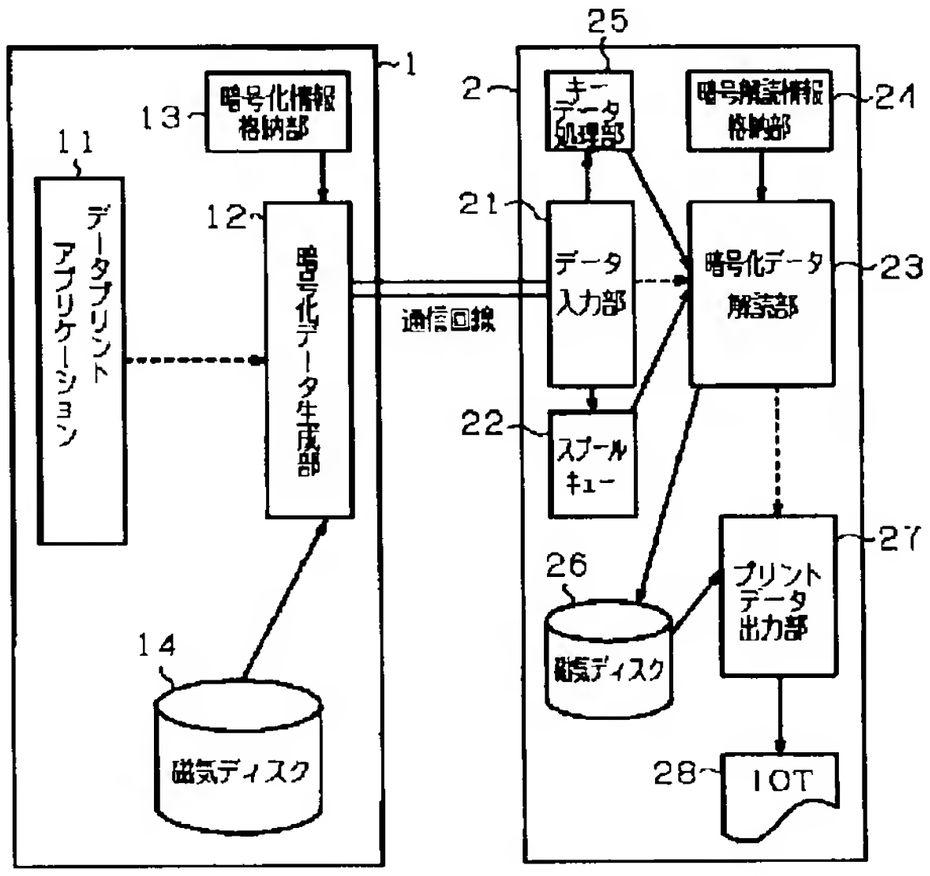
(74)代理人　弁理士　本庄　富雄　（外１名）

(54)【発明の名称】　プリントデータのセキュリティ方式

(57)【要約】

【目的】　スプールキューにセキュリティ対象データが存在していて、第三者がそれをディスプレー等を通して覗き見しようとしても、その内容を知られないようにして、セキュリティを確実に保つこと。

【構成】　プリントデータ生成装置１には、プリントデータを暗号化すると共に、暗号化データにユーザＩＤ，キーコード，暗号化ＩＤを付加してプリンタ側に転送する暗号化データ生成部１２を設ける。プリンタ２には、上記ユーザＩＤ等に基づいて、上記暗号化データを解読する暗号化データ解読部２３を設ける。プリンタ２に転送された暗号化データは、一旦スプールキュー２２に格納され、プリントする際には、パスワードが一致した時のみ、暗号化データ解読部２３で暗号解読しながら出力する。スプールキュー２２に格納されるのは、暗号化データであるので、その内容を覗き見されたとしても、見えるのは意味のないデータの塊であり、プリントデータの内容は知られずに済む。



1

【特許請求の範囲】
【請求項１】　プリントデータ生成装置は、プリントデータを暗号化すると共に、暗号化したプリントデータにユーザＩＤ，キーコード，暗号化ＩＤを付加してプリンタに転送する暗号化データ生成部を有し、プリンタは、転送された暗号化データを格納するスプールキューと、パスワードの一致を確認した上で上記スプールキューから暗号化データを取り出し、それを上記ユーザＩＤ，キーコード，暗号化ＩＤに基づいて解読し、解読したデータをプリントデータ出力側に送る暗号化データ解読部を有することを特徴とするプリントデータのセキュリティ方式。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、プリンティングシステムにおけるプリントデータのセキュリティ方式に関するものである。
【０００２】
【従来の技術】図１０は、ネットワークにホストコンピュータ及びプリンタが接続された状態を示す図である。図１０において、１００はネットワーク、１０１～１０５はプリンタ、１１１～１１３はホストコンピュータである。プリンタ１０１～１０５は、ネットワーク１００に接続され、そのネットワーク１００に接続された複数のホストコンピュータ１１１～１１３からの出力データを印刷する。
【０００３】このようにプリンタが複数の利用者で共用される場合、そのまま外部に出力させるのではプリントされた出力データが第三者の目に触れる可能性があり、機密が保持できない。そのため、機密を保持できるような対策を施したプリントデータのセキュリティ方式が従来から提案されている。従来の一般的なプリントデータのセキュリティ方式では、プリンタに対して、通常のプリントデータをパスワード付で転送する。プリンタ側では、転送されてきたプリントデータをパスワードと共にスプールキューに保持しておく。そして、それをプリントする際には、操作者に対してパスワードを要求し、入力されたパスワードと保持しておいたパスワードとが一致したときのみプリントを実行するようにして、セキュリティを確保するようにしている。
【０００４】なお、このようなプリントデータのセキュリティ方式に関連する従来の文献としては、例えば、特開昭６１－２６９７２９号公報，特開昭６２－３３２２号公報，特開平１－１５９７２４号公報等がある。
【０００５】
【発明が解決しようとする課題】
（問題点）しかしながら、前記した従来の技術には、スプールキュー内にプリントデータが存在する場合、第三者がディスプレー等を通してその内容を見ることができ、データの機密を確実に保持することはできないという問題点があった。

2

【０００６】（問題点の説明）従来の方式では、パスワードを知っていない限り、そのデータをプリントすることはできないが、プリントデータ自体は通常のデータである。したがって、それがスプールキュー内に保持されている時、見ようと思えば、プリンタに接続されているディスプレーを通してデータの中身を見ることは可能である。そのため、データの機密を確実には保持できない。本発明は、以上のような問題点を解決することを課題とするものである。
【０００７】
【課題を解決するための手段】前記課題を解決するため、本発明のプリントデータのセキュリティ方式では、プリントデータ生成装置は、プリントデータを暗号化すると共に、暗号化したプリントデータにユーザＩＤ，キーコード，暗号化ＩＤを付加してプリンタに転送する暗号化データ生成部を有し、プリンタは、転送された暗号化データを格納するスプールキューと、パスワードの一致を確認した上で上記スプールキューから暗号化データを取り出し、それを上記ユーザＩＤ，キーコード，暗号化ＩＤに基づいて解読し、解読したデータをプリントデータ出力側に送る暗号化データ解読部を設けることとした。
【０００８】
【作　　用】プリントデータ生成装置の暗号化データ生成部で、プリントデータは全て暗号化してからプリンタ側に転送する。一方、プリンタ側では、プリント出力するのはパスワードの一致を確認してからであるので、第三者がプリント出力するのを防止することができる。その上、暗号化されたプリントデータが解読されるのは、プリント出力する時であり、スプールキューには、転送されてきたデータがそのままの形で格納される。そのため、スプールキューにセキュリティ対象データが存在していても、そのデータは全て暗号化されていて、それをディスプレー等を通して見ようとしても、見えるのは何の意味も持たないデータの塊であり、第三者にその内容を知られることはない。したがって、データの機密が確実に保持できる。
【０００９】
【実施例】以下、本発明の実施例を図面に基づいて詳細に説明する。図１は、本発明の概要を示すブロック図である。図１において、１はプリントデータ生成装置、１１はデータプリントアプリケーション、１２は暗号化データ生成部、１３は暗号化情報格納部、１４は磁気ディスク、２はプリンタ、２１はデータ入力部、２２はスプールキュー、２３は暗号化データ解読部、２４は暗号解読情報格納部、２５はキーデータ処理部、２６は磁気ディスク、２７はプリントデータ出力部、２８は記録部である。
【００１０】プリントデータ生成装置１は、ホストコン

ピュータ，ワークステーション，パーソナルコンピュータ，ワードプロセッサ等の、プリントデータを生成する機能を有する装置である。生成されたプリントデータは、一旦磁気ディスク１４に格納される。データプリントアプリケーション１１は、暗号化データ生成部１２を起動させ、磁気ディスク１４に格納されているプリントデータの内、どのデータを処理するかを指示する。暗号化データ生成部１２は、暗号化情報格納部１３に格納されているキーコード，暗号化ＩＤ，暗号化手法等に基づいて、磁気ディスク１４に格納されているプリントデータを暗号化して、プリンタ２に転送する。

【００１１】プリンタ２のデータ入力部２１は、プリントデータ生成装置１から転送されたデータの内、暗号化データをスプールキュー２２に格納する。キーデータ処理部２５は、転送されたデータから、ユーザＩＤ，暗号化ＩＤ，キーコードを抜き出して保持する。暗号化データ解読部２３は、スプールキュー２２から暗号化データを受け取り、キーデータ処理部２５からそれに対応するユーザＩＤ，暗号化ＩＤ，キーコードを受け取り、さらに、暗号解読情報格納部２４から暗号解読手法等の暗号解読情報を受け取って、暗号化データを解読する。磁気ディスク２６は、解読された後のプリントデータを一時保持した後、プリントデータ出力部２７に引き渡す。

【００１２】図２は、暗号化情報格納部に格納されたデータの一例を示す図である。図２（イ）は、キーコード，暗号化ＩＤ格納テーブルであり、各ユーザＩＤ毎に、使用されるキーコードと暗号化ＩＤとを、それぞれ複数個ずつ格納している。図２（ロ）は、暗号化手法格納テーブルであり、各暗号化ＩＤに対応する暗号化手法を格納している。

【００１３】図３は、暗号解読情報格納部に格納されたデータの一例を示す図である。図３（イ）は、セキュリティ対象ユーザＩＤ格納部であり、プリントデータの機密を保持する必要のあるユーザのユーザＩＤを格納している。図３（ロ）は、ユーザＩＤ格納テーブルであり、各ログオンクラス毎に、そのログオンクラスでのプリント出力が許されるユーザのユーザＩＤを格納している。図３（ハ）は、暗号解読手法格納テーブルであり、各暗号化ＩＤに対応する暗号解読手法を格納している。これらの暗号解読手法は、図２（ロ）の暗号化手法格納テーブルに格納されている暗号化手法と１対１に対応している。なお、上記「ログオンクラス」とは、プリンタを操作する際にアクセスできるファイルや起動できるプログラムを、ユーザに応じて区別するためのものであり、通常、上位のログオンクラスに指定されたユーザほどアクセスできるファイルや起動できるプログラムの数は多くなる。

【００１４】次に、プリントデータ生成装置１からプリンタ２に転送するデータの内容を説明する。図４は、本発明による転送データフォーマットの一例を示す図である。このデータは、プリントデータ生成装置１の暗号化データ生成部１２で生成されるが、暗号化データにユーザＩＤ，暗号化ＩＤ，キーコードが付加される。

【００１５】次に、本発明の動作をフローチャートを参照しながら説明する。なお、プリントデータ生成装置１における暗号化情報格納部１３、及び、プリンタ２における暗号解読情報格納部２４の各データは、予め設定されているものとする。先ず、プリントデータ生成装置１の暗号化データ生成部１２において、プリントデータを暗号化してプリンタ２に転送する手順を説明する。

【００１６】図５は、プリントデータを暗号化して転送する手順の一例を示すフローチャートである。

ステップ１…ユーザが入力したユーザＩＤを転送データのＡの箇所（図４参照。以下、同様）にセットする。

ステップ２…暗号化情報格納部１３のキーコード，暗号化ＩＤ格納テーブル（図２（イ）参照）中の上記ユーザＩＤに対応する複数のキーコードの中から、１つをランダムに選定して、転送データのＣの箇所にセットする。

ステップ３…暗号化情報格納部１３のキーコード，暗号化ＩＤ格納テーブル（同上）中の上記ユーザＩＤに対応する複数の暗号化ＩＤの中から、１つをランダムに選定して、転送データのＢの箇所にセットする。

【００１７】ステップ４…データプリントアプリケーション１１によって指定されたプリントデータを、磁気ディスク１４から読み込む。

ステップ５…暗号化情報格納部１３の暗号化手法格納テーブル（図２（ロ）参照）中の、ステップ３で選定した暗号化ＩＤに対応する暗号化手法に基づいて、プリントデータの暗号化を行う。

ステップ６…暗号化データを転送データのＤの箇所にセットして、データをプリンタ２に転送する。

【００１８】次に、プリンタ２の暗号化データ解読部２３において、暗号化データを解読してプリントを開始させる手順を説明する。この手順は、プリント出力させようとする操作者が、プリントするデータ及びログオンクラスを指定してから開始される。図６は、暗号化データを解読してプリントを開始させる手順の一例を示すフローチャートである。

ステップ１…キーデータ処理部２５から、プリントするデータに対応するユーザＩＤを取得する。

ステップ２…暗号解読情報格納部２４のユーザＩＤ格納テーブル（図３（ロ）参照）中の、操作者が指定したログオンクラスに対応するユーザＩＤの中にステップ１で取得したユーザＩＤが有るか否かを調べる。

ステップ３…ない時、そのユーザに対して当該ログオンクラスでのプリントが許可されていないということになる。そこで、ログオンクラスの変更を促すメッセージをプリンタに接続されているディスプレーに表示し、入力を待つ。

ステップ４…暗号解読情報格納部２４のユーザＩＤ格納

テーブル（同上）中の、変更されたログオンクラスに対応するユーザＩＤの中にステップ１で取得したユーザＩＤが有るか否かを調べる。
ステップ５…ない時、変更されたログオンクラスでもプリントが許可されていないということになる。その時は、プリンタに接続されているディスプレーにエラー表示をして、プリントすることなく処理を終了する。
【００１９】ステップ６…ステップ２，ステップ４でユーザＩＤがあった時、暗号解読情報格納部２４のセキュリティ対象ユーザＩＤ格納部（図３（イ）参照）の中にステップ１で取得したユーザＩＤが有るか否かを調べる。
ステップ７…あれば、プリントデータの機密を保持する必要があるということになる。そこで、現在プリントしようとしている操作者がプリントデータを送ってきたユーザ本人であるか否かを確認するため、操作者に対してパスワードの入力を促すメッセージをプリンタに接続されているディスプレーに表示し、入力を待つ。
ステップ８…入力されたパスワードが予め登録されていたものと一致したか否かを判別する。
ステップ９…一致したら、キーデータ処理部２５から暗号化ＩＤを取得する。
ステップ１０…続いて、キーデータ処理部２５からキーコードを取得する。
ステップ１１…暗号解読情報格納部２４の暗号解読手法格納テーブル（図３（ハ）参照）から、ステップ９で取得した暗号化ＩＤに対応する暗号解読手法を取得する。
ステップ１２…暗号化データの解読を行う。
ステップ１３…解読したプリントデータを磁気ディスク２６を介してプリントデータ出力部２７に送って、プリントを開始させる。
【００２０】このようにすれば、先ず、パスワードによって、第三者がプリント出力するのを防止することができる。その上、スプールキューに格納されるデータは暗号化データであるので、スプールキューにセキュリティデータが存在していても、そのデータは全て暗号化されていて、それをディスプレー等を通して見ようとしても、見えるのは何の意味も持たないデータの塊であり、第三者にその内容を知られる恐れはない。その結果、データの機密が確実に保持される。また、パスワードだけでなく、ログオンクラスとの組合せによりプリント出力の可否を判定するようにしているので、より高度のセキュリティを確保できる。さらに、暗号化手法及びキーコードを複数の中からランダムに１つを選定するようにしているので、同じデータの暗号化でも１回目と２回目の暗号化データが同一になる確率は低くなり、データの隠蔽がより高度なものとなる。
【００２１】上記実施例では、ステップ４で、ログオンクラスが変更されても、それに対応するユーザＩＤの中にステップ１で取得したユーザＩＤがなかった時、あるいは、ステップ８で、パスワードが一致しなかった時、エラー表示を行って、プリントはしないようにしていた。しかし、そのような時、エラー表示を行うことなく、暗号化されたデータをそのまま印刷するようにすることもできる。図７は、暗号化データを解読してプリントを開始させる手順の他の例を示すフローチャートである。このフローチャートは、ステップ４，ステップ７でＮＯと判定された時、図６のフローチャートにおけるステップ５（エラー表示）を省略し、ステップ１２（プリント開始）を実行するようにしている点だけが、図６のものと相違しており、その他の手順は同じである。このようにすれば、例えば、パスワードが一致しなくてもプリントは実行されるが、暗号解読が行われないままプリント出力されるため、出力されるデータは意味不明のものとなり、プリントデータの機密は保持される。
【００２２】以上の実施例では、転送データフォーマット中のユーザＩＤは、個人に対応するものであった。しかし、それをグループに対応させて取り扱うようにすることもできる。図８は、暗号化情報格納部に格納されたデータの他の例を示す図であり、図９は、暗号解読情報格納部に格納されたデータの他の例を示す図である。図８（イ）は、グループユーザＩＤ格納テーブルであり、各グループユーザＩＤ毎に、そのグループに属するユーザＩＤが格納されている。図８（ロ），図８（ハ）は、図２（イ），図２（ロ）と同様なテーブルである。また、図９（イ），図９（ロ），図９（ハ）は、図３（イ），図３（ロ），図３（ハ）と同様の内容であるが、ただ、図９（ロ）のユーザＩＤ格納テーブルの中に、ユーザＩＤと共に、グループユーザＩＤも設定されている点で異なっている。
【００２３】すなわち、図８，図９のものが、図２，図３のものと異なる点は、プリントデータ生成装置１側において、複数のユーザＩＤに対して、グループユーザＩＤを定義する点である。また、プリンタ２側においても、各ログオンクラスにて、グループユーザＩＤの設定も行っている点である。
【００２４】この場合、プリントデータ生成装置１において、処理を行う際に入力するＩＤとしては、やはりユーザＩＤを入力する。ユーザＩＤが入力されると、図８（イ）のグループユーザＩＤ格納テーブルに基づいて、当該ユーザが属するグループユーザＩＤが取得される。そして、転送データのＡの箇所（図４参照）には、そのグループユーザＩＤがセットされる。転送データのＢ，Ｃの箇所には、それぞれ、ユーザＩＤに対応する暗号化ＩＤ及びキーコードがセットされる。プリンタ２側において暗号解読を行うに際しては、グループユーザＩＤは、ユーザＩＤと同等に取り扱われる。
【００２５】また、図１０に示したように、ネットワーク上に複数のホストコンピュータ１１１～１１３とプリンタ１０１～１０５が接続されている場合に、ユーザＩ

Ｄの代わりに、各ホストコンピュータのマシンＩＤを用いて、ホストコンピュータ単位でのプリント可否を設定することもできる。その場合、必ずしも、ホストコンピュータとマシンＩＤとが１対１に対応する必要はなく、複数のホストコンピュータに対して、１つのマシンＩＤを与えるようにしても差し支えない。

【００２６】

【発明の効果】以上述べた如く、本発明のプリントデータのセキュリティ方式によれば、次のような効果を奏する。先ず、パスワードによって、第三者がプリント出力するのを防止することができる。その上、スプールキューに格納されるデータは暗号化データであるので、スプールキューにセキュリティデータが存在していても、そのデータは全て暗号化されていて、それをディスプレー等を通して見ようとしても、第三者にその内容を知られる恐れはなく、データの機密が確実に保持される。また、実施例で行ったように、パスワードだけでなく、ログオンクラスとの組合せによりプリント出力の可否を判定するようにすれば、より高度のセキュリティを確保できる。さらに、暗号化手法及びキーコードを複数の中からランダムに１つを選定するようにすれば、同じデータの暗号化でも１回目と２回目の暗号化データが同一になる確率は低くなり、データの隠蔽がより高度なものとなる。

【図面の簡単な説明】

【図１】　本発明の概要を示すブロック図

【図２】　暗号化情報格納部に格納されたデータの一例＊を示す図

【図３】　暗号解読情報格納部に格納されたデータの一例を示す図

【図４】　本発明による転送データフォーマットの一例を示す図

【図５】　プリントデータを暗号化して転送する手順の一例を示すフローチャート

【図６】　暗号化データを解読してプリントを開始させる手順の一例を示すフローチャート

【図７】　暗号化データを解読してプリントを開始させる手順の他の例を示すフローチャート

【図８】　暗号化情報格納部に格納されたデータの他の例を示す図

【図９】　暗号解読情報格納部に格納されたデータの他の例を示す図

【図１０】　ネットワークにホストコンピュータ及びプリンタが接続された状態を示す図

【符号の説明】

１…プリントデータ生成装置、１１…データプリントアプリケーション、１２…暗号化データ生成部、１３…暗号化情報格納部、１４…磁気ディスク、２…プリンタ、２１…データ入力部、２２…スプールキュー、２３…暗号化データ解読部、２４…暗号解読情報格納部、２５…キーデータ処理部、２６…磁気ディスク、２７…プリントデータ出力部、２８…記録部、１００…ネットワーク、１０１～１０５…プリンタ、１１１～１１３…ホストコンピュータ

【図２】

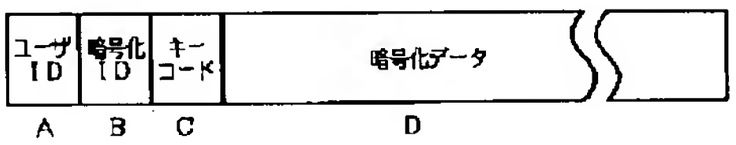
(イ)

	ユーザＩＤ	キーコード	暗号化ＩＤ
1	ＩＤ1	K1,K2,K3	1，3，5
2	ＩＤ2	K4,K5,K6	2，4
3	ＩＤ3	K7,K8,K9	2，3，4
⋮	⋮	⋮	⋮
n	ＩＤn	K10,K11,K12	1，3

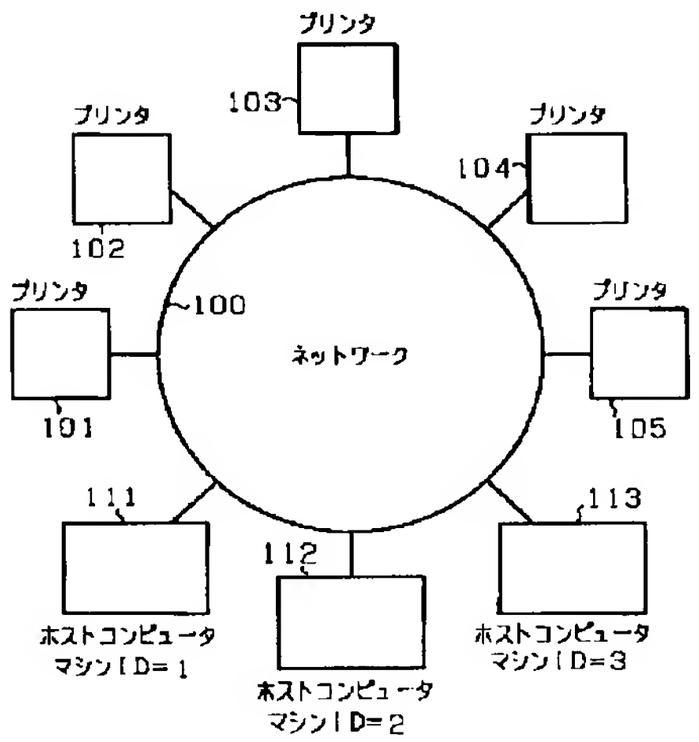
(ロ)

暗号化ＩＤ	暗号化手法
1	手法１
2	手法２
3	手法３
4	手法４
5	手法５

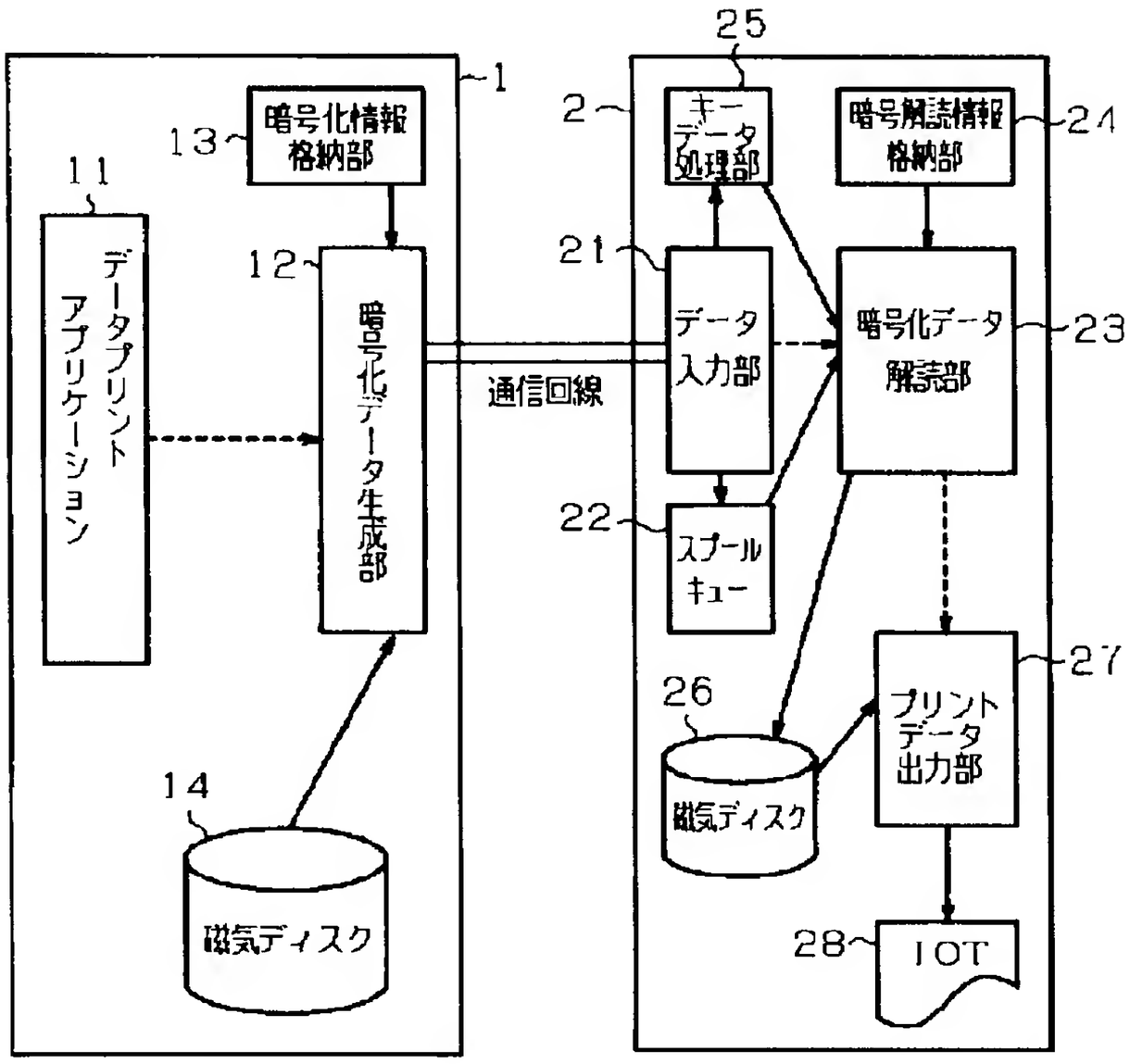
【図４】



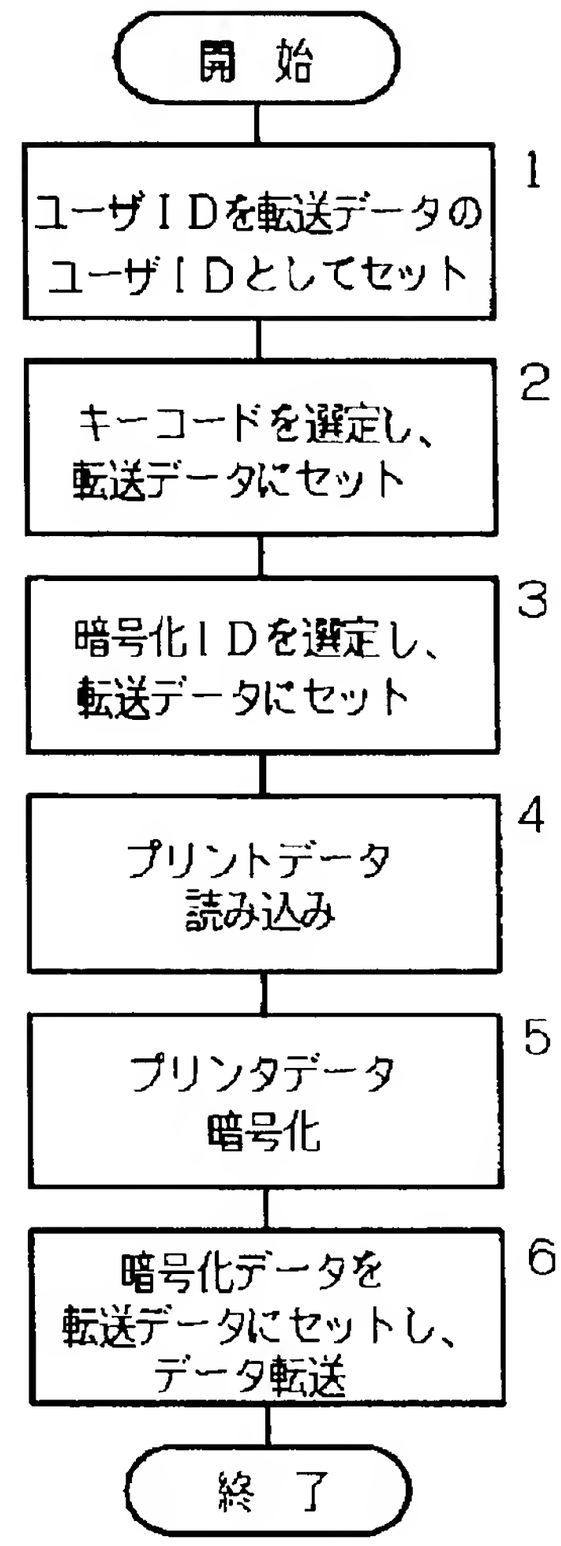
【図１０】



【図１】



【図５】



【図３】

セキュリティ対象ユーザＩＤ
ＩＤ１，ＩＤ２， ＩＤ４，ＩＤ７

（イ）

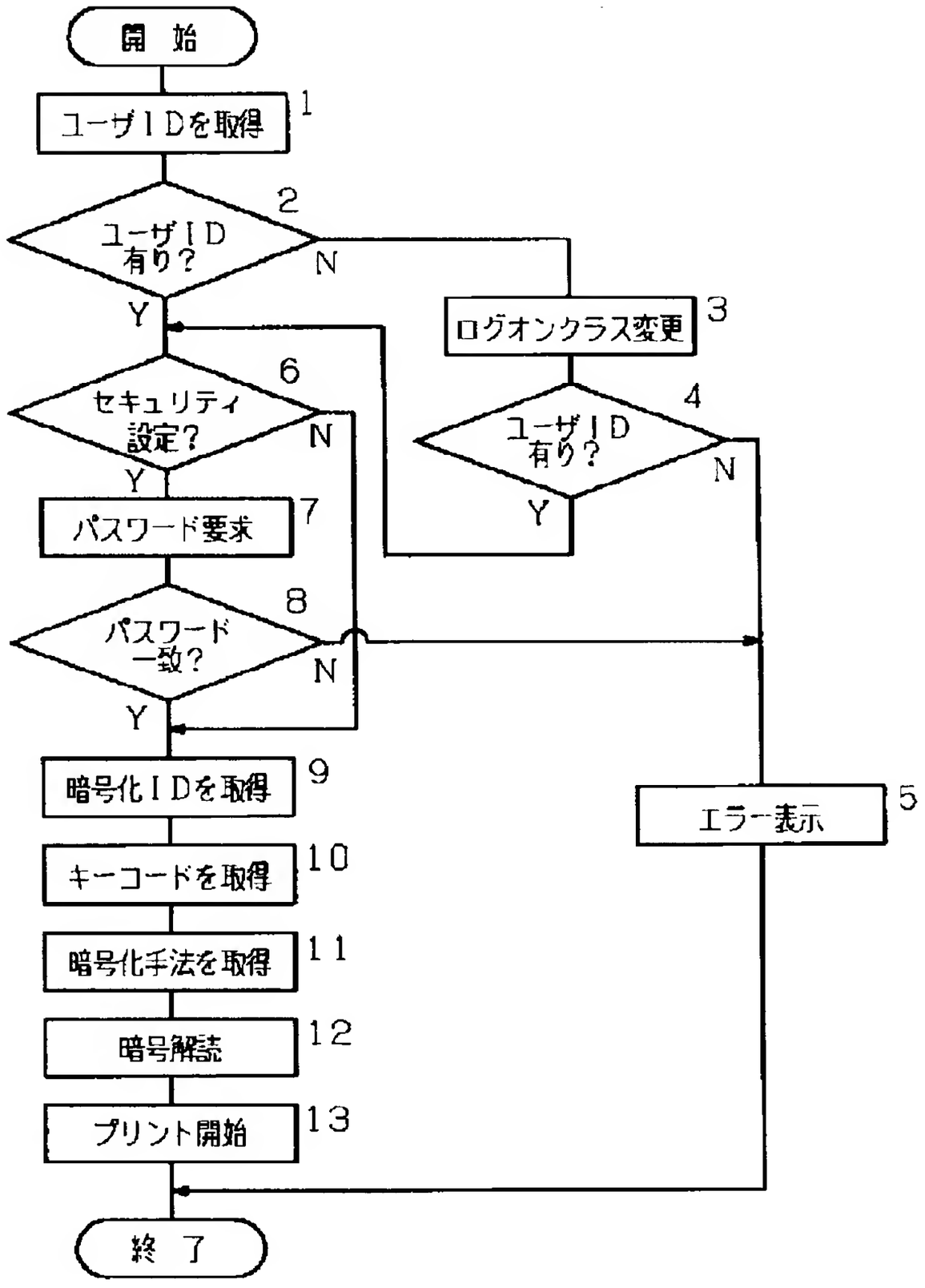
ログオンクラス	ユーザＩＤ
1	ＩＤ１，ＩＤ２，ＩＤ３
2	ＩＤ４，ＩＤ５
3	ＩＤ６，ＩＤ７
⋮	⋮
N	ＩＤｎ

（ロ）

暗号化ＩＤ	暗号解読手法
1	解読手法１
2	解読手法２
3	解読手法３
4	解読手法４
5	解読手法５

（ハ）

【図６】



【図９】

セキュリティ対象ユーザＩＤ
ＩＤ１，ＩＤ２，ＩＤ４，ＧＩ２

（イ）

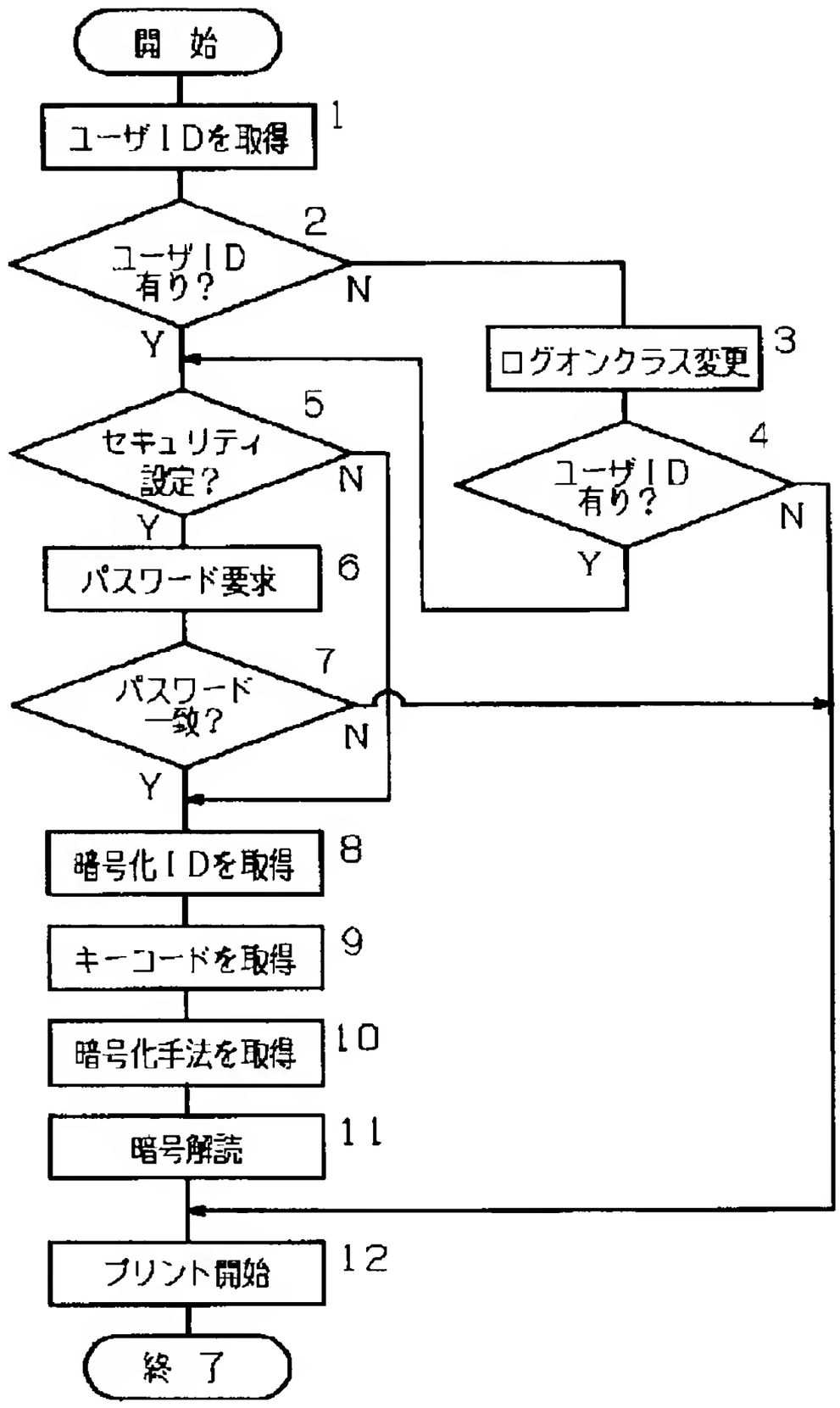
ログオンクラス	ユーザＩＤ
1	ＩＤ１，ＩＤ２，ＩＤ３
2	ＩＤ４，ＩＤ５
3	ＧＩ１
4	ＧＩ２
⋮	⋮
N	ＩＤｎ

（ロ）

暗号化ＩＤ	暗号解読手法
1	解読手法１
2	解読手法２
3	解読手法３
4	解読手法４
5	解読手法５

（ハ）

【図７】


開　始
ユーザＩＤを取得
1
ユーザＩＤ
有り？
2
N
Y
ログオンクラス変更
3
ユーザＩＤ
有り？
4
N
Y
セキュリティ
設定？
5
N
Y
パスワード要求
6
パスワード
一致？
7
N
Y
暗号化ＩＤを取得
8
キーコードを取得
9
暗号化手法を取得
10
暗号解読
11
プリント開始
12
終　了

【図８】

	グループユーザＩＤ	ユーザＩＤ
1	GID_1	UID_1, UID_2, UID_3
2	GID_2	UID_4, UID_5, UID_6
⋮	⋮	⋮
L	GID_L	——, UID_L

(イ)

	ユーザＩＤ	キーコード	暗号化ＩＤ
1	UID_1	K_1, K_2, K_3	1, 3, 5
2	UID_2	K_4, K_5, K_6	2, 4
3	UID_3	K_7, K_8, K_9	2, 3, 4
⋮	⋮	⋮	⋮
n	UID_n	K_{10}, K_{11}, K_{12}	1, 3

(ロ)

暗号化ＩＤ	暗号化手法
1	手法１
2	手法２
3	手法３
4	手法４
5	手法５

(ハ)